

WK:ELM
F. #2018R01268

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

-----X

UNITED STATES OF AMERICA

- against -

TAEGYUN KIM, M.D.,

Defendant.

-----X

TO BE FILED UNDER SEAL

COMPLAINT AND AFFIDAVIT IN
SUPPORT OF APPLICATION FOR
ARREST AND SEARCH WARRANTS

19-M- 280

(T. 18, U.S.C., § 1347)

IN THE MATTER OF AN APPLICATION OF
THE UNITED STATES OF AMERICA FOR A
SEARCH WARRANT FOR THE PREMISES
KNOWN AND DESCRIBED AS 141-47
NORTHERN BOULEVARD, QUEENS, NEW
YORK AND ALL ELECTRONIC DEVICE
AND LOCKED AND CLOSED
CONTAINERS FOUND THEREIN

-----X

EASTERN DISTRICT OF NEW YORK, SS:

RYAN HODKINSON, being duly sworn, deposes and states that he is a
Special Agent with the United States Department of Health and Human Services, Office of
the Inspector General ("HHS-OIG"), duly appointed according to law and acting as such.

On or about and between June 2016 and the present, within the Eastern
District of New York, the defendant TAEGYUN KIM, M.D., did knowingly and willfully
execute, and attempt to execute, a scheme and artifice to defraud a healthcare benefit
program affecting commerce, as defined in Title 18, United States Code, Section 24(b), that
is, Medicare, and did obtain and attempt to obtain by means of false and fraudulent pretenses,

representations and promises, money and property owned by, and under the custody and control of, said health care benefit program, in connection with the delivery of and payment for healthcare benefits, items and services.

(Title 18, United States Code, Section 1347)

Upon information and belief, there is probable cause to believe that there is located in 141-47 NORTHERN BOULEVARD, QUEENS, NEW YORK AND ELECTRONIC DEVICES AND LOCKED AND CLOSED CONTAINERS FOUND THERE (the "SUBJECT PREMISES") evidence, fruits and/or instrumentalities of healthcare fraud and attempted healthcare fraud, in violation of 18 U.S.C. § 1347.

The source of your deponent's information and the grounds for his belief are as follows:

1. I have been a Special Agent with HHS-OIG for approximately 13 months. Previously, I worked as an auditor for HHS Office of Audit Services for approximately seven years. I am currently assigned to investigate fraud involving federal healthcare programs, including schemes to defraud Medicare and Medicaid. During my tenure at HHS-OIG, I have participated in a variety of criminal healthcare fraud investigations, during the course of which I have interviewed witnesses, conducting physical surveillance, executed search warrants, reviewed documents and records – including Medicare claims data, bank records, phone records, Medicare beneficiaries' medical records, invoices, and other records. I am familiar with the records and documents maintained by healthcare providers and the laws and regulations related to administration of the Medicare program. Through my training, education and experience, I am familiar with the techniques

and methods of operation used by individuals involved in criminal healthcare fraud to conceal their activities and avoid detection by law enforcement.

2. Among other duties, I am currently participating in an investigation of violations of, among other things, 18 U.S.C. § 1347 by TAEGYUN KIM, M.D. ("KIM"). Specifically, the investigation is focused on a scheme involving the fraudulent submission of claims for reimbursement to Medicare for healthcare services that were not in fact provided.

3. I make this Affidavit in support of an application for an arrest warrant for KIM and for a search warrants to search the SUBJECT PREMISES, as more fully described in Attachment A. Based on the facts set forth in this Affidavit, I respectfully submit that there is probable cause to believe that there presently is located in the SUBJECT PREMISES certain items and property, which are more fully set forth in Attachment B, which constitute evidence, fruits and instrumentalities of healthcare fraud and attempted healthcare fraud, in violation of 18 U.S.C. § 1347.

4. The facts and information contained in this Affidavit are based upon my own participation in the investigation, discussions with other federal law enforcement officers, records discovered in the course of this investigation that have been reviewed by myself and other law enforcement officers, my training and experience, and interviews with various individuals, including Medicare beneficiaries and KIM himself.¹ I am also familiar with the investigation described in part below through analysis of reports submitted by other law enforcement personnel.

¹ Because the purpose of this Affidavit is to set forth only those facts necessary to establish probable cause to arrest KIM and search the SUBJECT PREMISES, I have not described all the relevant facts and circumstances of which I am aware.

PROBABLE CAUSE

I. The Defendant and Subject Premises

5. The defendant TAEGYUN KIM, M.D., is a medical doctor who is licensed to practice in the state of New York, and who has been licensed to practice in the state of New York since in or about November 2011. KIM specializes in internal medicine. He resides in Flushing, Queens in New York.

6. KIM maintains an office at 141-47 Northern Boulevard, Suite 2R, in Flushing, Queens, New York (the SUBJECT PREMISES). Law enforcement officers conducted surveillance of SUBJECT PREMISES on January 9, 2019, March 11, 2019, March 12, 2019; and March 13, 2019. Law enforcement officers also visited the SUBJECT PREMISES on March 26, 2019, and determined that the office remains in operation. A photograph of the front door of the building where the SUBJECT PREMISES is located is included below and in Attachment A. The office is located on the second floor of a four-story, multi-unit building with a gray stone façade depicted in the photograph below. There are two suites per floor in the building. KIM's office is Suite 2R, located on the second floor. KIM's name is on the door leading into Suite 2R. The office space within Suite 2R consists of a reception and waiting area, two examination rooms and KIM's office. The office has a large window facing Northern Boulevard with white English- and Korean-language lettering identifying the office on the window and a sign with Korean-language lettering identifying the office hanging above the window.



II. Relevant Background

A. The Medicare Program

7. Medicare is a federal health insurance program for people who are 65 years of age or older, or certain younger people with disabilities or certain specified illnesses. People who received benefits under Medicare are referred to Medicare “beneficiaries.” Medicare is a “health care benefit program” as defined by 18 U.S.C. § 24(b).

8. Medicare is administered by the Centers for Medicare and Medicaid Services ("CMS"). CMS is a federal agency within the United States Department of Health and Human Services. CMS contracts with other entities to administer Medicare in different regions or states. National Government Services, Inc. ("NGS") is the CMS contractor responsible for administering Medicare in New York state.

9. Healthcare providers certified to participate in Medicare are assigned a provider transaction access number (a "PTAN") for billing purposes. After a healthcare provider renders a service for a Medicare beneficiary, the provider uses their PTAN, along with other information, to submit a claim for payment to the Medicare contractor or carrier assigned to administer the program in the provider's state. Providers working in New York state submit their claims for payment to NGS.

10. In order to receive payment for a service covered by Medicare, the healthcare provider must submit a claim for payment electronically or in writing. The claim must include, among other information: information identifying the provider; the physician providing the service; information identifying the patient; the services provided; the diagnosis or nature of the illness or condition treated; and the date or dates of service. The claim identifies the service provided by reference to codes set forth in the Healthcare Common Procedure Coding System ("HCPCS Codes"). The HCPCS Codes are monitored by CMS. There are two levels of HCPCS codes. The first level, Current Procedural Terminology codes ("Level I HCPCS Codes" or "CPT Codes"), are comprised of five numerical digits and are contained in the Healthcare Common Procedure Coding System book, which is published by the American Medical Association. CPT Codes identify

medical services and procedures ordered by physicians or other licensed healthcare providers.

11. Medicare will reimburse providers for certain surgical procedures on the musculoskeletal system performed on beneficiaries, including, as relevant here:

CPT Code	Description of Procedure
20610	Aspiration ² from, or injection into, a major joint (defined as a shoulder, hip, knee, or subacromial bursa), or both aspiration and injection of the same joint
20611	Aspiration from, or injection into, a major joint or joint capsule with recording and reporting using ultrasound guidance

12. In submitting a claim to Medicare for these and other procedures, a healthcare provider certifies, among other things, that the services were actually provided to the patient-beneficiary, and that the services were medically necessary.

13. CMS contracts with SafeGuard Services LLC (“SGS”) to perform a number of functions focused on maintaining the integrity of Medicare, along with other federal health insurance programs. SGS is the Northeastern United Program Integrity Contractor (“NE UPIC”) responsible for fraud, waste and abuse detection, deterrence and prevention activities in the Northeast, including in the state of New York. Among other things, SGS analyzes billing data, identifies issues or problems with specific healthcare providers, conducts investigations and research into potentially fraudulent Medicare providers, and, where appropriate, refers cases for administrative proceedings or to law enforcement in order to address fraud, waste and abuse.

²

Here, the term “aspiration” refers to the removal of fluid.

III. The Fraudulent Scheme

14. Under 18 U.S.C. § 1347, it is illegal to knowingly and willfully execute and attempt to execute a scheme and artifice to defraud Medicare and to obtain and attempt to obtain, by means of false and fraudulent pretenses, representations and promises, money and property owned by and under the custody and control of Medicare in connection with the delivery of and payment for healthcare benefits, items and services. There is probable cause to believe that KIM has engaged in violations of 18 U.S.C. § 1347. Specifically, as described below, there is probable cause to believe that KIM, while practicing medicine in Queens, New York, engaged in a scheme to submit claims for payment to Medicare for surgical procedures that were not performed.

15. Specifically, KIM has submitted claims to Medicare seeking payment for joint aspirations – a procedure in which a sterile needle and syringe are used to drain synovial fluid from a patient's joint – or joint injections with the assistance of ultrasound technology, when, in fact, he was not assisted by ultrasound technology during these procedures. Physicians are compensated at a higher rate for joint aspirations or injections performed with the aid of ultrasound technology than they are for aspirations or injections performed without the aid of ultrasound technology.

16. According to Medicare enrollment documents bearing KIM's signature, KIM is medical doctor. He is licensed to practice in the state of New York. The enrollment documents identify the SUBJECT PREMISES as the location where KIM practices medicine.

IV. CMS Audit

17. On June 5, 2018, representatives from SGS conducted an on-site visit to KIM's office – the SUBJECT PREMISES – in order to conduct an audit of KIM's Medicare billing. During the visit, KIM signed a document attesting that all of the information included therein was true and complete (the "Attestation"). In the Attestation, KIM stated that he was the owner of and sole practitioner rendering services in the medical offices located at the SUBJECT PREMISES. KIM stated that he took handwritten notes regarding the treatment he provided to individual patients. KIM attested that he submitted claims to Medicare on his own behalf, based off the handwritten notes he took during patient consultations. KIM further attested that, if Medicare requested documentation in support of those claims, KIM retroactively created records in the EMR in order to satisfy the request.

18. In response to questioning from the SGS auditors, KIM attested that he typically did not use ultrasound guidance when he aspirated or injected joints. He stated that he was sufficiently experienced in performing joint aspirations and injections, and did not need the assistance of ultrasound technology.

19. The SGS auditors requested medical records for 82 Medicare beneficiaries medical records for dates of service between July 1, 2016 and December 30, 2017. KIM provided the SGS auditors with medical records for eight patients at the time of June 5, 2018 on-site visit, and agreed that he would provide the remaining records within 30 days. KIM's Attestation provided that KIM used an electronic medical records system (the "EMR"), and that he was the only person in his practice who had access to the EMR. KIM also attested that he did not regularly enter the information collected in his handwritten notes

into that system at the time of the SGS interview, and had not done so in approximately three years.

20. KIM provided SGS with medical records of 81 beneficiaries on August 6, 2018, more than 60 days after the date of the on-site visit. At the same time, KIM resubmitted documentation for seven of the eight beneficiaries whose records he previously provided on June 5, 2018. SGS compared the records provided by KIM on June 5, 2018 to those records provided by KIM on August 6, 2018. The records provided on August 6, 2018, included a number of additions and edits that were not present in the records provided on June 5, 2018, including, among other information:

a. Additional purported patient-beneficiary complaints were added to the "Chief Complaint" section of the majority of the medical records provided on August 6, 2018, such as a notation that the patient-beneficiary was suffering increased urinary frequency and urgency, while the records provided on June 5, 2018, merely specified that the patient-beneficiaries were visiting for "med refills/bp check up;"³

b. The records provided on August 6, 2018, were altered to indicate that KIM had measured the patient-beneficiaries' vital signs (such as the patient-beneficiary's blood pressure), whereas the documentation provided on June 5, 2018 stated that no vital sign measurements were taken;

³ Based on my training and experience, I understand the notation "med refills/bp check up" to mean that the patient was visiting to obtain a refill prescription for medication and have his or her blood pressure checked.

c. Additional information was added the records provided on August 6, 2018, including KIM's assessment of the patient-beneficiaries' conditions and treatment plan, which had been absent from the records provided on June 5, 2018; and

d. The records provided on August 6, 2018 included KIM's signature stamp, whereas there was no signature included in the medical records submitted on June 5, 2017.

21. Based on the inconsistencies between the medical records KIM provided on June 5, 2018 and those he provided on August 6, 2018, and between the medical records and the statements KIM made in the Attestation, the SGS auditors concluded that changes had been made to KIM's medical records in order to support his claims to Medicare for services rendered.

V. March 26, 2019 Visit to the Subject Premises

22. On March 26, 2019, federal law enforcement officers with HHS-OIG and the FDA visited the SUBJECT PREMISES at approximately 10:45 a.m. The office was open and several patients were on-site at the time. When they arrived, the law enforcement officers informed the receptionist that they were there from HHS and asked to speak to KIM.

23. When asked, KIM stated that he personally does all of his medical billing, including the submission of claims through Medicare, using electronic medical billing software. KIM stated that he enters the billing information at his office – the SUBJECT PREMISES – on the computer. The law enforcement officers observed two desktop computers at the SUBJECT PREMISES, one in the reception area and one in KIM's office.

VI. Patient Interviews

24. Law enforcement officers reviewed claims submitted by KIM for joint aspiration procedures, and have conducted interviews of several Medicare beneficiaries identified by KIM as having received such procedures.

A. Patient Number One

25. Patient Number One, an individual whose identity is known to me, is a female Medicare beneficiary who has been identified in claims submitted for reimbursement to Medicare as someone for whom KIM has billed healthcare services between June 2016 and December 2017. Law enforcement officers interviewed Patient Number One at her home on January 18, 2019. Patient Number One confirmed that KIM was her doctor between 2016 and June 2018.

26. During the interview, Patient Number One stated that she received an injection in her knees approximately every month during that time period from KIM. Patient Number One did not recall KIM using ultrasound technology in connection with the injections she received, although she thought it was possible that he used it on her first visit. Patient Number One stated that KIM did not take any notes during her visits with him.

27. According to claims submitted by KIM, KIM performed 23 procedures for Patient Number One during that time period, including: seven procedures billed to Medicare between June 2016 and March 2017 using CPT Code 20610, referring to aspiration from, or injection into, a major joint; and 16 procedures billed to Medicare between March 2017 and December 2017 using CPT Code 20611, referring to aspiration from, or injection into, a major joint or joint capsule with the assistance of ultrasound technology. Contrary to the facts provided by Patient Number One, KIM's claims to Medicare indicated that KIM

used ultrasound technology to assist in most of the injections he provided to Patient Number One, and frequently used ultrasound technology during Patient Number One's later visits.

B. Patient Number Two

28. Patient Number Two, an individual whose identity is known to me, is a female Medicare beneficiary who has been identified in claims submitted for reimbursement to Medicare as someone for whom KIM has billed healthcare services between December 2016 and May 2018. Law enforcement officers interviewed Patient Number Two by phone on January 18, 2019. Patient Number Two stated that KIM was her doctor.

29. During the interview, Patient Number Two stated that she received an injection in an alternate knee approximately every four months from KIM. Patient Number Two additionally stated that she was referred to KIM by a friend, who told Patient Number Two that KIM would give her a lot of injections. Patient Number Two informed the officers that her last visit to KIM was in August 2018, and that she received her last injection in her knees in the fall of 2017. Patient Number Two described to the officers that she received one ultrasound in connection with the knee injections early in her treatment by KIM, but did not receive additional ultrasounds moving forward.

30. According to claims submitted by KIM, KIM performed 23 procedures for Patient Number One during that time period, including: four procedures billed to Medicare in December 2016 using CPT Code 20610, referring to aspiration from, or injection into, a major joint; and 35 procedures billed to Medicare between March 2017 and May 2018, using CPT Code 20611, referring to aspiration from, or injection into, a major joint or joint capsule with the assistance of ultrasound technology. Contrary to the facts provided by Patient Number Two, KIM's claims to Medicare indicated that KIM used

ultrasound technology to assist in most of the injections he provided to Patient Number Two, and frequently used ultrasound technology during Patient Number Two's later visits.

Additionally, KIM's claims to Medicare indicated that he performed 35 injections on Patient Number Two's knees in the fourteen-month period between March 2017 and May 2018, over ten times as many injections than the approximately three injections annually reported by Patient Number Two. Finally, KIM's claims to Medicare indicated that he performed ten injections on Patient Number Two's knees – all with the aid of ultrasound technology – between February 2018 and May 2018, while Patient Number Two reported that KIM had not provided Patient Number Two with any injections in her knees since late 2017.

C. Patient Number Three

31. Patient Number Three, an individual whose identity is known to me, is a female Medicare beneficiary who has been identified in claims submitted for reimbursement to Medicare as someone for whom KIM has billed healthcare services between March 2017 and April 2018. Law enforcement officers interviewed Patient Number Three by phone on January 18, 2019. Patient Number Three confirmed that KIM was her doctor.

32. During the interview, Patient Number Three stated that she saw KIM as her primary doctor, and consults with him concerning blood tests, acute illness and general questions concerning her health. Patient Number Three provided that she did not consult KIM concerning her joints, and had never received an injection in her joints from KIM. At the time of the interview, Patient Number Three indicated that she remained a patient of KIM. However, she specified that she receives knee injections from a different physician.

33. According to claims submitted by KIM, KIM performed 11 procedures for Patient Number Three during that time period, all of which were billed to Medicare between March 2017 and April 2018 using CPT Code 20611, referring to aspiration from, or injection into, a major joint or joint capsule with the assistance of ultrasound technology. Contrary to the facts reported by Patient Number Three – that KIM had never performed any injections on her knees – KIM's claims to Medicare indicated that KIM performed 11 injections in Patient Number Three's joints over the course of approximately one year.

D. Patient Number Four

34. Patient Number Four, an individual whose identity is known to me, is a female Medicare beneficiary who has been identified in claims submitted for reimbursement to Medicare as someone for whom KIM has billed healthcare services between June 2018 and April 2018 (together with Patient Number One, Patient Number Two and Patient Number Three, the "Patients"). Law enforcement officers interviewed Patient Number Four at her home on January 18, 2019. Patient Number Four confirmed that KIM was her doctor.

35. During the interview, Patient Number Four stated that she received an injection in each of her knees approximately every six months from KIM. Patient Number Four informed the officers that she received one ultrasound in connection with the knee injections in 2018, but did not receive any other ultrasounds in connection with her treatment by KIM.

36. According to claims submitted by KIM, KIM performed 14 procedures for Patient Number Four during that time period, including: five procedures billed to Medicare between June 2016 and December 2016 using CPT Code 20610, referring to aspiration from, or injection into, a major joint; and nine procedures billed to Medicare

between February 2017 and April 2018, using CPT Code 20611, referring to aspiration from, or injection into, a major joint or joint capsule with the assistance of ultrasound technology. Contrary to the facts provided by Patient Number Four, KIM's claims to Medicare indicated that KIM claimed to have used ultrasound technology to assist in the majority of the injections he provided to Patient Number Four, and frequently used ultrasound technology during Patient Number Four's later visits. Additionally, KIM's claims to Medicare indicated that he performed 14 injections on Patient Number Four's knees in the approximately two-year period between June 2016 and April 2018, nearly twice as many injections than the approximately four injections annually reported by Patient Number Four.

37. As to each of the Patients, KIM submitted a claim for payment of \$74.00 to Medicare and received a payment of \$55.32 for each claim for a joint aspiration without the use of ultrasound technology (under CPT Code 20610). KIM submitted a claim for payment of \$110.00 to Medicare and received a payment of \$83.70 for each claim for a joint aspiration with the use ultrasound technology (under CPT Code 20611).

38. Based on my training and experience – including my participation in this investigation – I have learned that individuals who engage in fraudulent conduct like the scheme described herein often keep physical evidence, fruits, and instrumentalities of their crimes inside their offices, including, in this case: both falsified and accurate medical records for patients; medical billing records⁴; documents identifying the procedures, if any, that were

⁴ Based on the investigation, it is my belief that KIM maintains his patient's medical records and his medical billing records on the desktop computers in his office space. Among other things, on March 26, 2019, KIM informed law enforcement officers that he maintains his patient medical records and medical billing records himself on his office computers through electronic medical records and billing software.

actually performed on their patients; and ledgers or other records recording payments made or received in furtherance of the scheme. I have also learned that such office spaces will also include evidence of the healthcare providers using the office to practice medicine.

39. Additionally, I have learned through my training, education and experience that such evidence, fruits and instrumentalities are often stored in locked containers, safes, secret compartments, closets, drawers, above or below ceiling and floor tiles, behind false walls and, when digital in nature, inside locked or lockable electronic devices (e.g., computers and smart telephones) and in other places intended to avoid detection by other people, including law enforcement.

40. Accordingly, and based on all of the above, I submit that there is probable cause to believe that the SUBJECT PREMISES, and any closed and/or locked containers found therein, will contain evidence, fruits and instrumentalities of the healthcare fraud and attempted healthcare fraud, in violation of 18 U.S.C. § 1347, and the SUBJECT PREMISES; and any closed and/or locked containers found therein, will also contain electronic devices that will contain (and will, in and of themselves, constitute) further evidence, fruits and instrumentalities of the healthcare fraud.

TECHNICAL TERMS

41. Based on my training and experience, I use the following technical terms to convey the following meanings:

(a) Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

(b) Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS

42. As described above and in Attachment B, this application seeks permission to search for certain documents and records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

43. *Probable cause.* I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

(a) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

(b) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

(c) Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

(d) Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

44. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

(a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a

file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

(b) As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain

information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

(c) A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

(d) The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

(e) Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

45. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

(a) The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

(b) Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

(c) Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

46. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the law enforcement officers executing this warrant to image, or otherwise copy, storage media that reasonably appear to

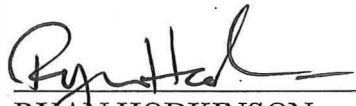
contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant. In the event that the law enforcement officers executing the warrant are unable to image, or otherwise copy, storage media encompassed by the warrant on-site, the warrant I am applying for would permit law enforcement officers executing the warrant to seize such storage media for a reasonable amount of time, in order to complete the imaging, or other copying, process at an off-site location.

REQUEST FOR SEALING

47. I respectfully request that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application, arrest warrants and search warrant. I believe that sealing these documents is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be arrested or searched at this time. Based upon my training and experience, I have learned that online criminals actively search for law enforcement affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through various forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

CONCLUSION

WHEREFORE, your deponent respectfully requests that a warrant be issued for the arrest of defendant TAEGYUN KIM, M.D., so that he may be dealt with according to law. I further respectfully request that a warrant be issued, pursuant to Federal Rule of Criminal Procedure 41, to search the SUBJECT PREMISES, as further described in Attachment A, and to seize those items set forth in Attachment B, that may constitute evidence, fruits and instrumentalities of violations of 18 U.S.C. § 1347.



RYAN HODKINSON
Special Agent, HHS-OIG

Sworn to before me this
21 day of March, 2019

S/ Lois Bloom

THE HONORABLE LOIS BLOOM
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to be Searched

The property to be searched is a physician's office located at 141-47 Northern Boulevard, Suite 2R, Flushing, Queens in New York, and electronic devices and all locked and closed containers found therein (the "Subject Premises"). The Subject Premises is located on the second floor of a four-story, multi-unit building with a gray stone façade. There are two suites per floor in the building. The Subject Premises is Suite 2R, located on the second floor. Taegyun Kim's name is on the door leading into Suite 2R.



ATTACHMENT B*Property to be Seized*

1. All items, including documents, records, evidence, fruits and instrumentalities, relating to violations of 18 U.S.C. § 1347, those violations involving TAEGYUN KIM, M.D., and occurring after June 1, 2016, including but not limited to:

- (a) Documents constituting, concerning, or relating to patient files, bills, invoices and claims for payment or reimbursement for services billed, provided, or alleged to have been provided to patients to include, but not limited to, reimbursement claim forms, explanations of medical benefits, dispensing orders, detailed written orders or prescriptions, certificates of medical necessity, information from physician(s) concerning the patients' diagnosis, superbills or "face sheets" indicating what procedures were performed for particular patients, and proof of delivery of services and/or items that were submitted by KIM or any representative acting on behalf of KIM;
- (b) All contracts, agreements, papers, and affiliated records constituting, concerning, or relating to the provision of medical services or prescription medication by KIM or any representative acting on his behalf, including but not limited to, manufacturer catalogs, purchase orders, invoices, and receipts;
- (c) All letters constituting, concerning, or relating to efforts to collect co-payments and/or deductibles for individuals who may have received health care services from KIM;
- (d) All correspondence and cancelled checks relating to notice of overpayment and request for refunds from Medicare or any other health insurance provider concerning KIM;
- (e) All correspondence to and from Medicare or any other health insurance provider concerning KIM, including, but not limited to, manuals, advisories, newsletters, bulletins and publications;
- (f) Financial books and records and documents constituting, concerning or relating to KIM, including but not limited to: bank accounts, money market accounts, checking accounts, investment accounts, securities accounts, 401k funds, mutual funds, retirement funds, and credit accounts, including deposits, disbursement, cancelled checks, draft electronic transfers, ledgers, loan statements, and loan agreements;
- (g) All contracts, agreements, logs, lists or papers affiliated with any medical

professional services, referrals, or storage for KIM;

- (h) All employee files and resumes relating to KIM, including but not limited to any handwritten or computerfiles listing any and all employee names, addresses, telephone numbers and background information for all current and former employees; and
- (i) All contracts, agreements or paper affiliated with any medical insurance billing company for KIM.

2. Computers or storage media used as a means to commit the violations described above, including healthcare fraud in violation of 18 U.S.C. § 1347.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- (a) evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- (b) evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- (c) evidence of the lack of such malicious software;
- (d) evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- (e) evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- (f) evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- (g) evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- (h) evidence of the times the COMPUTER was used;
- (i) passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

- (j) documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- (k) records of or information about Internet Protocol addresses used by the COMPUTER;
- (l) records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- (m) contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.